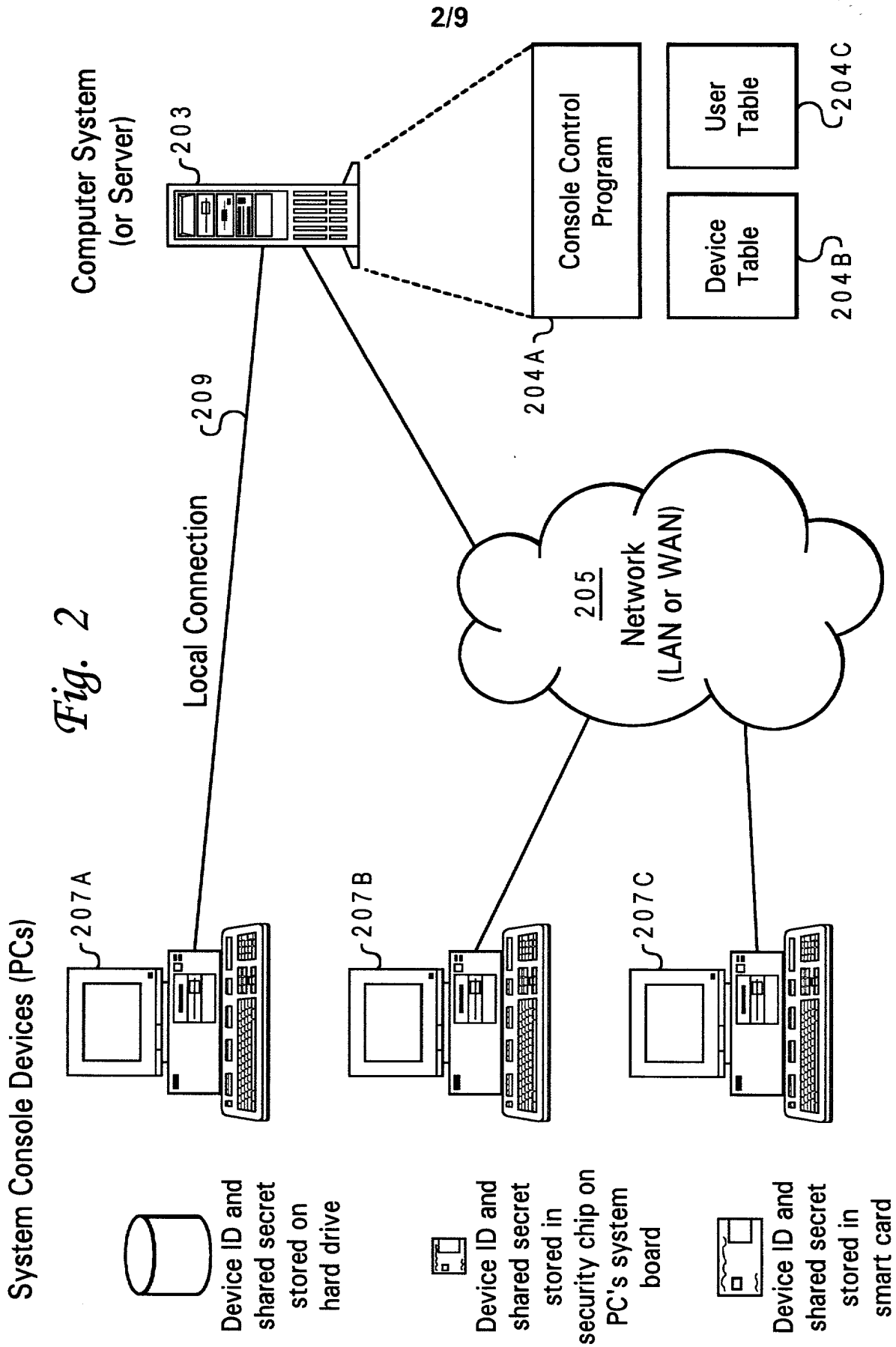


Fig. 1

FIG. 1



Console session flow

Normal flow -

Prompt for I_D , P_A , I_{Ux} , P_{Ux}

Setup wizard -

- 1) Prompt for I_D , P_D , P_A , I_{Ux} , P_{Ux}
- 2) Use PKCS-5 to encrypt P_D with P_A

Shipped with:

$I_D = QCONSOLE, H(P_D) = H(QCONSOLE)$

$I_{U3} = QSECOFR, H(P_{U3}) = H(QSECOFR)$

$I_{U2} = 22222222, H(P_{U2}) = H(22222222)$

$I_{U1} = 11111111, H(P_{U1}) = H(11111111)$

Derive K_D

Set $P_D = K_D$ if first use of P_D

Derive K_D

Set $H(P_D) = H(K_D)$

Derive K_U

Derive K_U

Legend:

I_D = Device identifier

P_D = Device shared secret

P_A = Access passphrase

I_{Ux} = User ID

P_{Ux} = User passphrase

K_D = Device session key

K_U = User session key

R = Random number

$H(x)$ = Hash of x

Device EKE flow with $H(P_D)$

User EKE flow with $H(P_U)$

Secure console session
Encrypted with K_U

NOTE: The first console session uses the well known shipped device identifier and user ID to access the iSeries. The device passphrase is modified in the initial flow ($P_D = K_D$). Therefore, the genesis device essentially "gets in free."

Fig. 3A

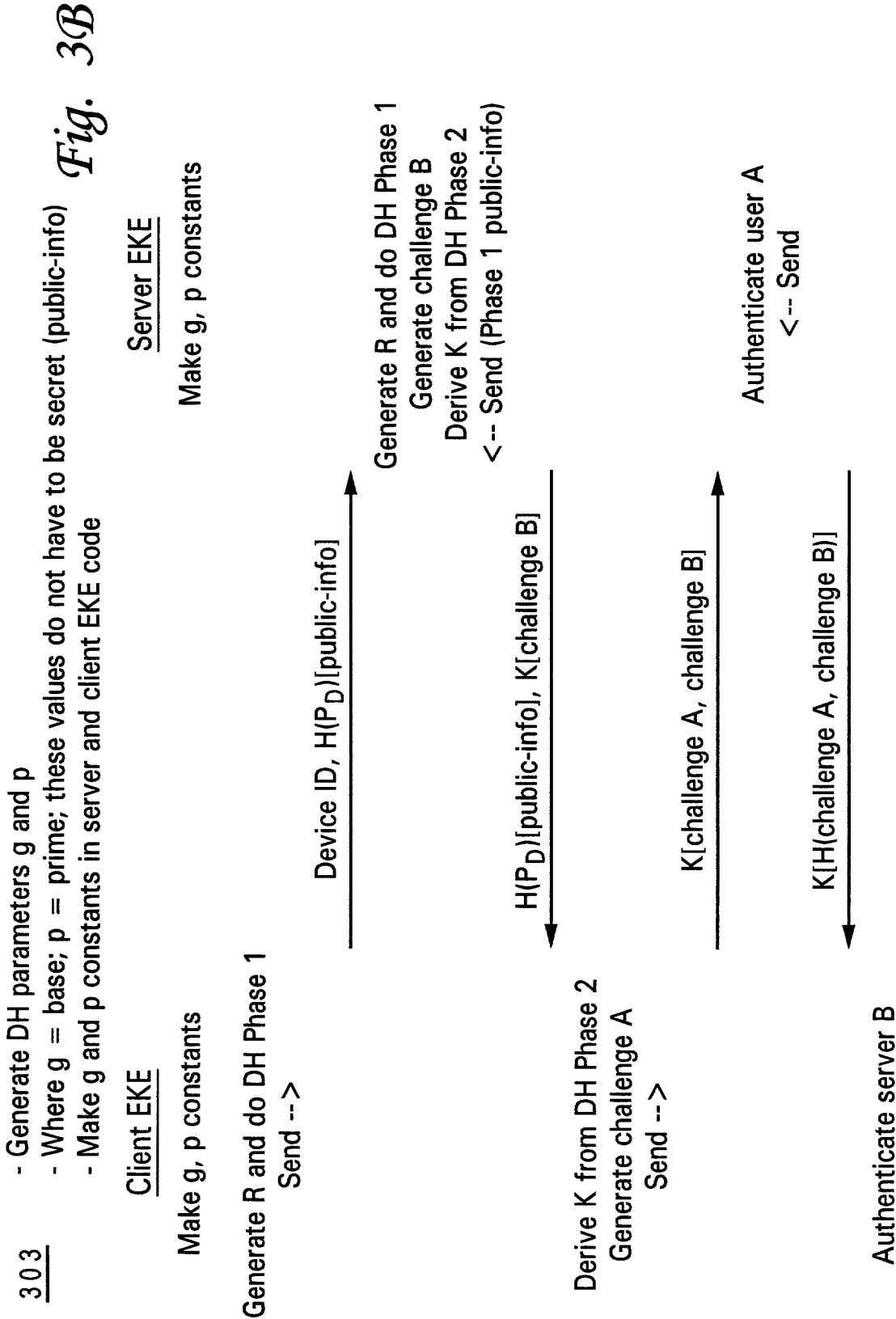


Fig. 3B

Refer to BSAFE Reference Manual for description of DH Phase 1 & 2.
NOTE: The challenge strings must be a different length than the encryption block.

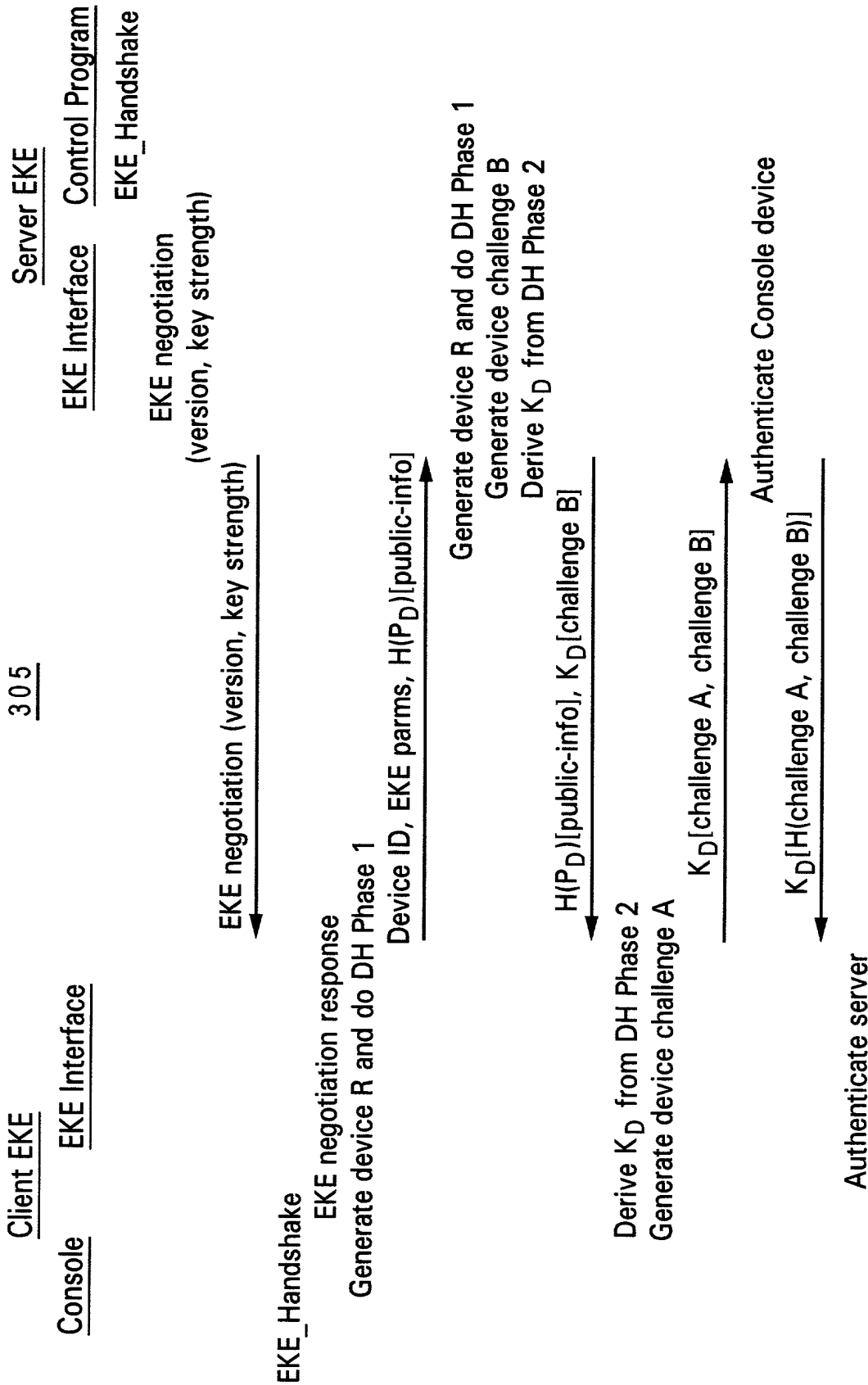
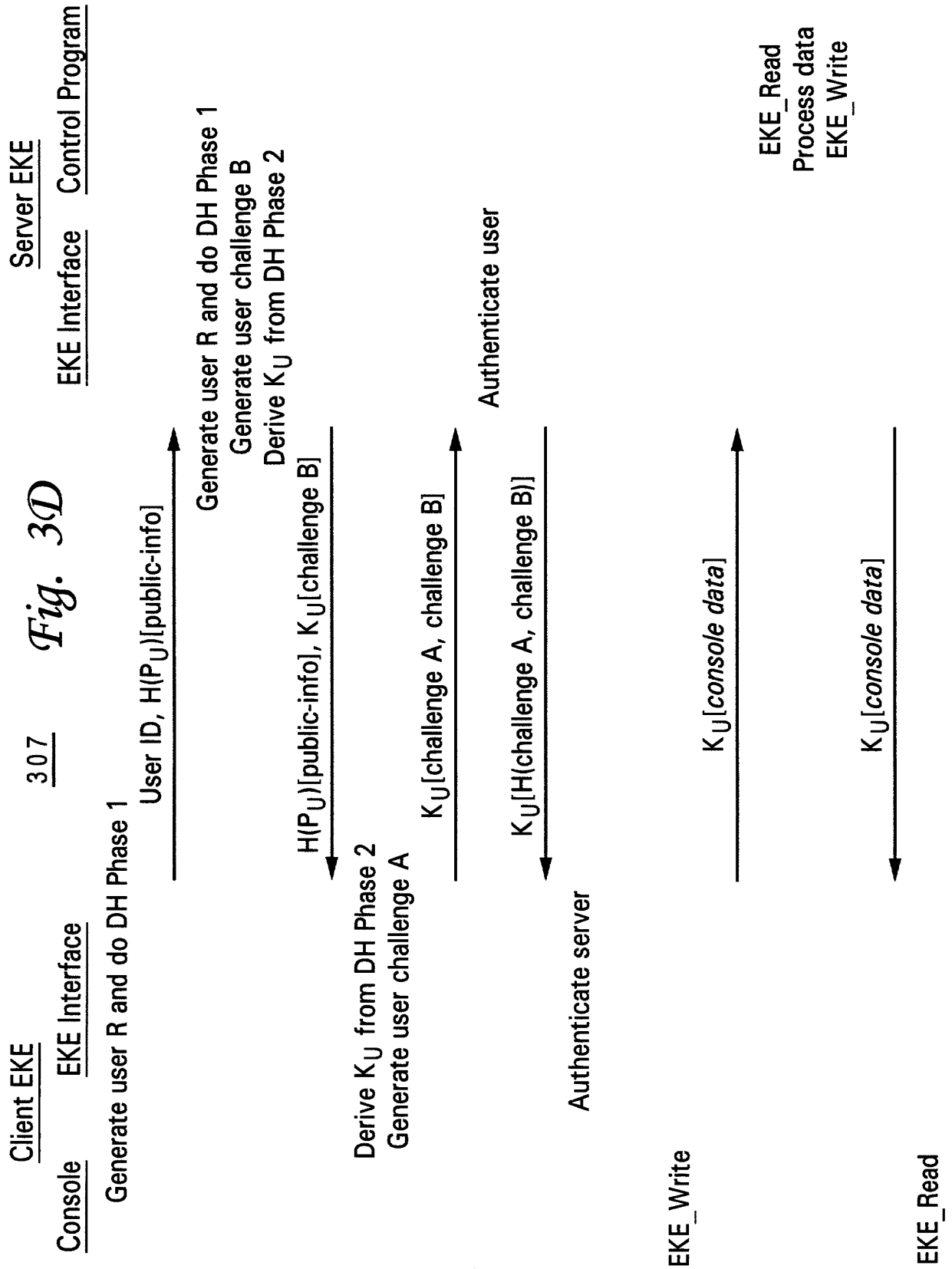
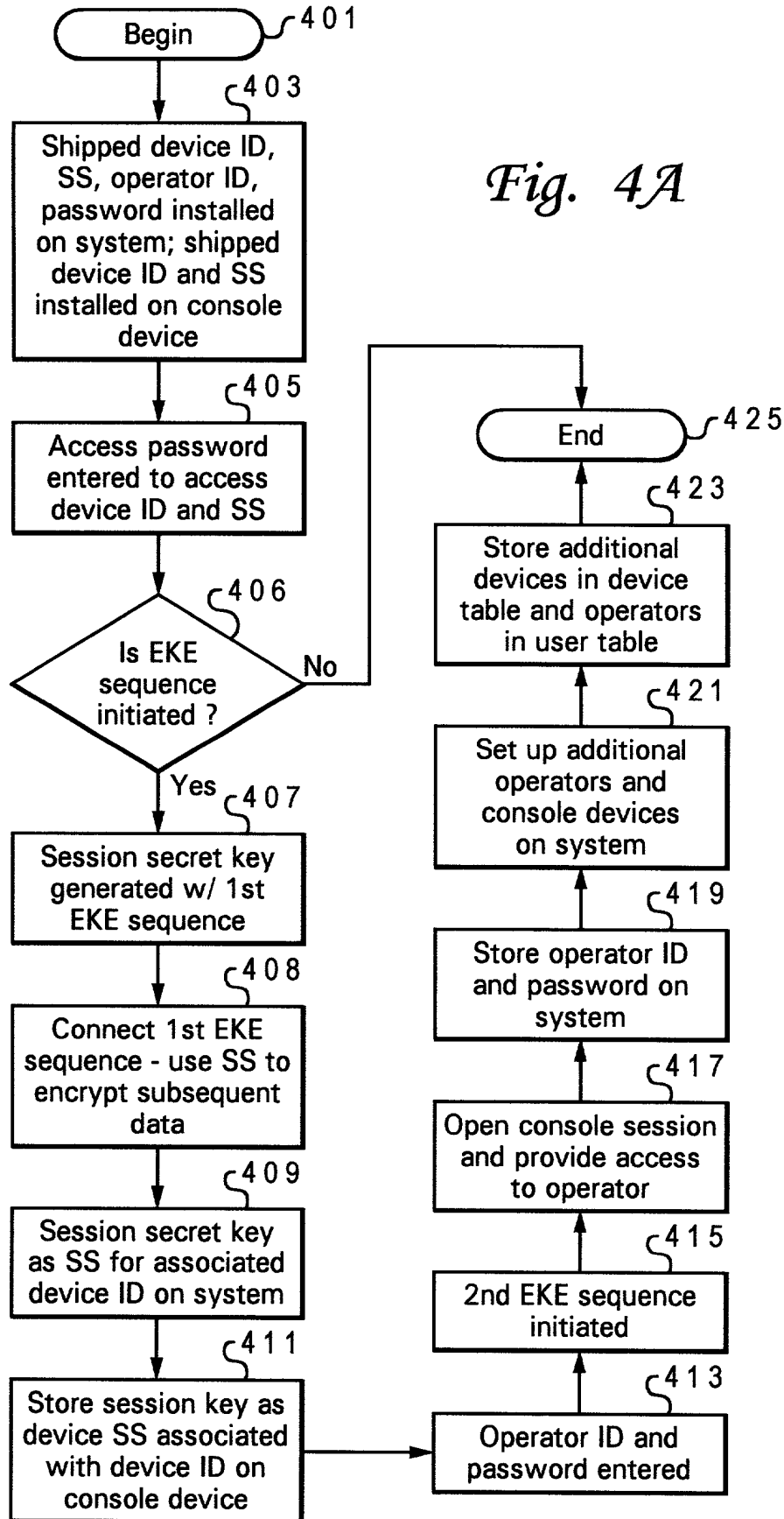


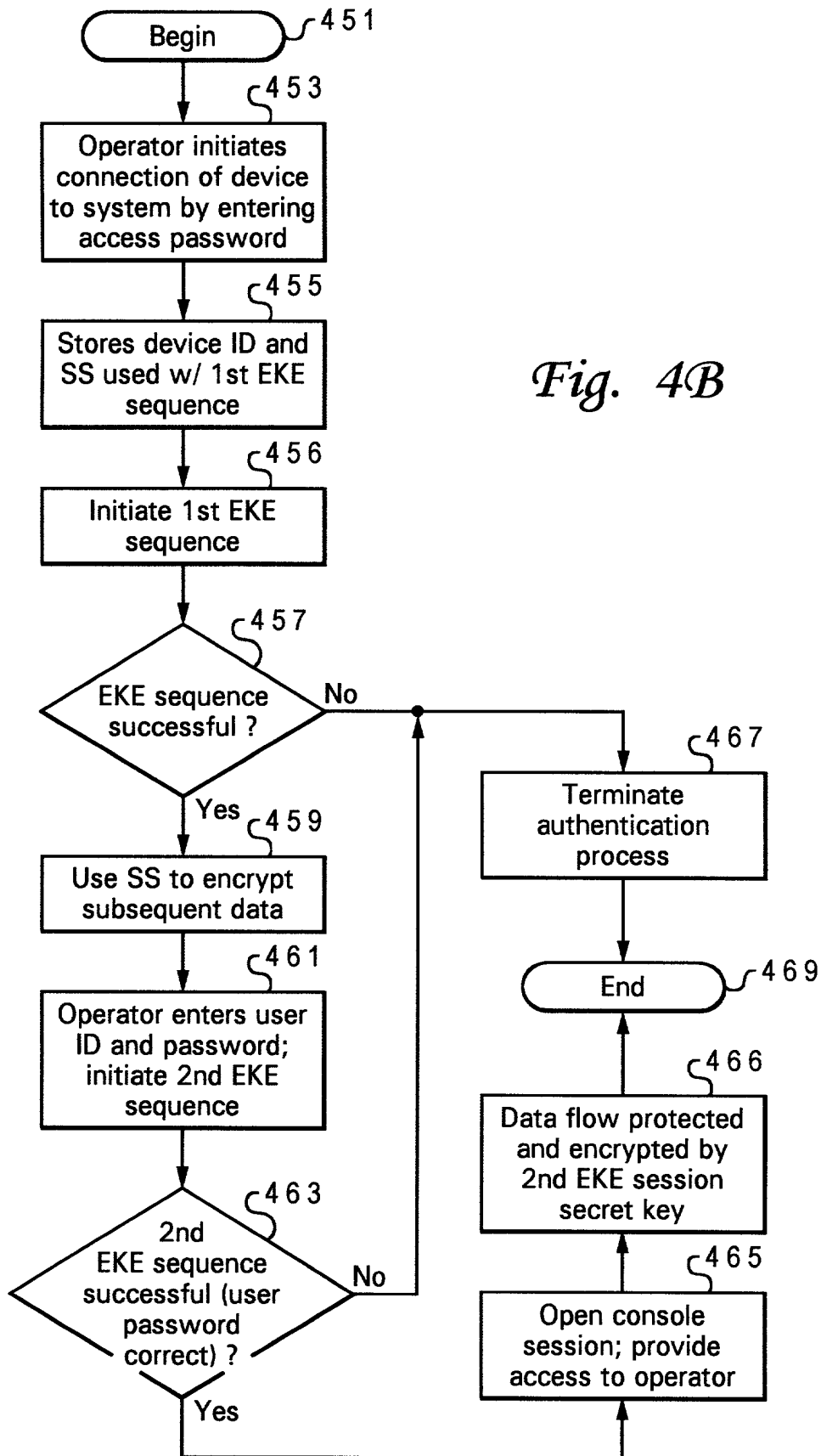
Fig. 3C

Pass 1 for device complete,
begin Pass 2 for user...





09828548-073001



09828548-073001

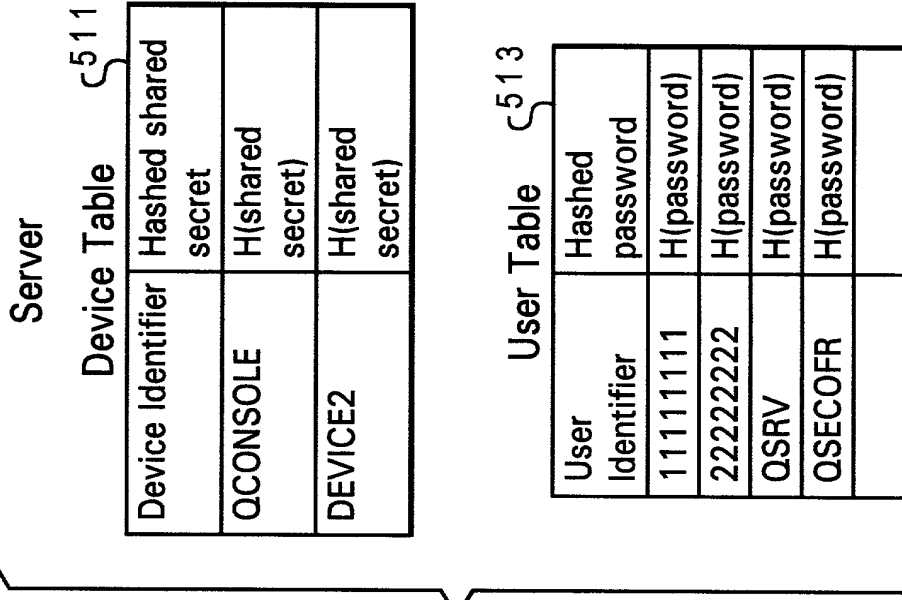


Fig. 5B

Client Device (PC) 501

Server Connection	
Server1	Hash (device identifier, shared secret)
Server2	Hash (device identifier, shared secret)

Fig. 5A